SKYDOGCON

2012 PROGRAM

WHY SKYDOGCON?

Thank you for attending SkyDogCon!

Skydog and company believe that the most interesting stuff happens when you bring together smart people in a relaxing environment. Everything about SkyDogCon is crafted to promote this belief. There is only one track, so you don't have to miss any of the amazing talks. The speakers that have been invited are some of the best and brightest in their respective fields. They were also chosen because they are enthusiastic and approachable, so feel free to buy them a beer and strike up a conversation. SkyDogCon is an environment where you can see what other people are working on, share your interests, and try things that are completely new. In between talks or when you have down time, check out the famous Expo area, where anyone can show off their projects and half-baked ideas. New this year is the Lockpick Village and Capture the Flag contest. Drop by each of these areas so you can legally learn how security systems, both physical and virtual, work and how they can be compromised.

Please; have a great time, challenge yourself, try something new and take advantage of this environment. A gathering of so many like-minded hackers and makers and curiosity seekers only happens once a year.

SKYDOGCON

DERBYCON

Hack3rCon^3
Doomsday Eve

Program printed Courtesy of Allen Printing, 415 Spence Lane, Nashville, TN
615-255-2078 - allenprinting.com

RULES OF ENGAGEMENT

We all sat around to come up with our "rules of the con". Here is what we came up with to share with you all, in no particular order.

1. Don't be a jerk - Self Explanatory
2. Have fun, but be reasonable - Remember that this is a conference at a hotel, NOT a frat house.
3. Listen to and be nice to the staff and agents - They are here to ensure that a good time is had by all.
4. Respect people's privacy - Do not take photos without permission

Any picture taken that involves people in the foreground in focus must be taken with their permission. If anyone complains to a staff member that you have taken their photo without permission, you will be asked to delete that photo. Please comply.

EVENTS

SkyDogCon Survival Guide

Thursday, October 25th at 6:00pm in the Pink Slip Lounge

The most common request from the attendees last year was a little time set aside for new con goers. Some people felt a little intimidated to come in to a group of hackers and not know exactly what to expect. This session is meant to give those new to SkyDogCon and the Hacker Con scene a few tips and an opportunity to ask questions in a small crowd. We will have a little time for a meet and greet with the SkyDogCon team as well as some time to get to know one another.

MexiCon World Tour Comedy Show

Thursday October 25th at 7:00pm in the Pink Slip Lounge

The only thing better than a comedy show is a hacker comedy show. Come laugh with the SkyDogCon team as we blow off a little steam and watch our favorite team member MadMex put on his "Con-Renowned" comedy routine. An hour-long string of stories that could only happen to, and be told by, a member of our community. Previously only seen in room parties at conferences like ShmooCon, DefCon, and OuterzOne, MadMex will string together some of his best stuff like "The Ambien Chronicles", "V is for Vasectomy" and "The TSA and teh Gay". We are honored to bring you MadMex in his live comedy club debut!

"Reboot" - Film Screening

Friday, October 26th at 8:45 in The Main Ballroom

SkyDogCon is proud to present a special screening of the new film "Reboot".

Set within a dystopian world that is a collision between technology and humanity, "Reboot" touches upon many of the current social and political concerns that arise as the physical becomes more and more intertwined with the virtual.

In contemporary Los Angeles, a young female hacker (Stat) awakens from unconsciousness to find an iPhone glued to her hand and a mysterious countdown ticking away on the display. Suffering from head trauma, and with little recollection of who she is or what is happening, Stat races against time to figure out what the code means, and what unknown event the pending zero-hour will bring.

Hacker Jeopardy

Friday, October 26 at 9:30pm in the Main Ballroom

If you like obscure technical references and the true stories behind major hacks you should definitely attend Hacker Jeopardy. For years one of the most popular events at DefCon, the legend finally comes to Nashville. Watch as teams match wits, skills and the limits of alcohol endurance to see who can keep on topic long enough to be crowned the winner. Brought to you by our friends Winn Schwartau and G Mark Hardy, the same duo that have made this game a classic will serve it up together again here at SkyDogCon. Teams of 4-6 individuals can apply, but must be over 21 and have their ID ready at the con. For more information and to sign up, email operations@skydogcon.com with the subject line "Hacker Jeopardy." Spaces are limited and demand is high so contact us today.

Musical Performance by Int0x80 of Dual Core

Saturday, October 27th at 9:00pm in The Main Ballroom

Back by popular demand, int0x80 will be performing again this year! Come out and check the mad skillz of one of the top nerdcore rappers in the hacking scene! As one half of the duo DualCore, int0x80 brings some intense energy and beats. This is a show nobody wants to miss. We are so happy to be hosting int0x80 as he is a long time friend and supporter of our community. Be sure to check out his music at dualcoremusic.com

Lockpick Village

Throughout the conference in the Lower Level - Create

Ever wondered how to pick a lock? Know how, but want to better your skills? Come out to the Lockpick Village and spend some time learning and practicing your craft. We have lockpickers at every skill level who are happy to show you the ropes. It is a great place to sit and relax and get to know your fellow attendees while learning valuable survival techniques/cool bar tricks.

Expo Area

Throughout the conference in Lower Level - Network

SkyDogCon will be hosting an expo area again this year where attendees can show off their ideas and projects to fellow attendees and to our sponsors. Come see what your friends are working on, share your thoughts and get inspired. We will be checking in throughout the conference to see all of the projects, both finished and in progress. On Sunday morning, we will announce an award to the most inventive or intriguing project. If you would like to present something in the expo area next year, contact operations@skydogcon.com, with the subject line "Expo." Pre- registration for the expo area is required in order to ensure that there is enough space for you and all of your projects.

Hardware Hacking Lab

All Day Friday and Saturday on the Lower Level - Network

We literally put weeks of work into the badge hanging around your neck. Why? Because it's a fully programmable development platform perfect for cool homebrew projects. The Hardware Hacking Lab has plenty of spare parts and gadgets to play with! We have some kits to build if you want to learn to solder, or if you're in the mood to make or modify something we have soldering stations and the like available for use.

Sponsor Area

Throughout the conference outside the Main Ballroom

Want to learn more about our sponsors? Check out the SkyDogCon Sponsor Area. Thanks to all our cool sponsors for making SkyDogCon possible.

Vendor Area

Throughout the conference in Ballroom IV

Check out the Vendor Area. Take a stroll through the space, pick up something new. Do you have design ideas? We have a vinyl cutter there ready for your creations. For the more adventurous, we also have a laser cutter/engraver. We can cut wood, acrylic, and even etch aluminum. See that Mac Book Pro in front of you? Want your logo/name engraved on it? Bring it!

LEGO(TM) Build Area

Throughout the conference in the Lower Level - Create

Got an inner child you need to let loose? Come to the LEGO™ table and show us your creation. Snap a photo and email it to operations@skydogcon.com with the subject line "LEGO." The most inventive use of LEGO™ will win the contest. The winner will be announced during closing ceremonies.

Crypto Challenge

Throughout the conference

GMark Hardy has agreed to create a crypto challenge exclusively for SkyDogCon this year! Can you crack the code?

2. 

Capture the Flag

Friday and Saturday October 26-27 on the Lower Level - Build

The best way to learn the techniques of modern attackers and defenders is to watch them in action during a Capture the Flag event. Teams must first attack and compromise an objective, and then defend it against other players.

This year's event is our most comprehensive to date. We're calling it "Duplicity CTF" and it involves both the physical and virtual space. Teams will need all sorts of capabilities including: lock picking, system admin, incident handling and forensics, physical penetration, wireless cracking, and good ole fashioned hacking. Bring all your snazzy tools: cables, pwn plugs, wireless cards, cool distros, network scanners, lock picks, cameras, motion detectors, and any other sneaky tricks you can think of. We'll have plenty of challenges for you to crack.

Here's how it works: each team of up to 6-10 individuals needs to register and will have to compete twice to win. As the red team, you'll have the opportunity to break into an office, gather information and use it to stage your attack. As the blue team, you'll have to protect the office and systems from the nefarious reds. Scoring will be based on the steps you take and how well you perform in the test. Never done something like this before? Don't worry! We'll have different level challenges for everyone.

Interested in participating next year? Email operations@skydogcon.com for more information with the subject line "DuplicityCTF" or follow on Twitter @DuplicityCTF.

6. 1337

Brad 'the nurse' Smith

All Weekend at Registration

On Thursday, October 27, 2011, our dear friend Brad Smith - nurse, computer smith, hacker extraordinaire, musician, chef, and all-round goofball - suffered a hemorrhagic stroke while giving a presentation at the Hacker Halted conference in Miami, some 2,500 miles away from his home in Montana. Thanks to the quick actions of several friends in the audience, he was rushed to the hospital where he had emergency brain surgery to stop the bleeding. He remained in a coma for 21 days. His wife Nina flew down to be by his side, and remained with him for the next four months as he was transferred to a V.A. rehab unit nearby. In March, he was strong enough to endure the plane trip home, and two friends from Helena were dispatched to assist in the transfer.

As we all know, being sick in America is not cheap or affordable. If you would like to make a contribution to help with Brad's ongoing medical expenses, send a check made out to Lost and Foundation, 517 Knight Street, Helena, MT 59601. Be sure to write the name "Brad Smith" on the memo line. Alternately, you can drop some $$$ into the donation jar at Registration. We'll be adding to it and sending more help their way. Thanks!

SPEAKERS & TALKS

Rious and Sachin

Hacking the SOC Badge

Forget high level languages. We hack the bare metal on a microcontroller with less than 1 MB of RAM, and we're lucky if we even get a watchdog timer. IF you know what an 8051 is, or want to, we'll show you where to start.

Rious spent most of his youth and spends much of his present spare time defeating physical security systems. Though now a Cisco and Novell certified engineer with a real job at a large, unnamed, national electronics company, Rious still finds time to wreak havoc on western (and occasionally eastern) Michigan.

Sachin has been building and hacking hardware as part of his day job for the past 16 years. He is employed at a prestigious university where he has designed things that have been launched into space and built instruments for clinical research. Sachin studied molecular biology in college and like a lot of people is doing something completely unrelated to his degree. He has taught himself biomedical engineering through a lot of trial and error. Like many of you, Sachin has been tearing apart toys of all kinds since he was a child, now he makes toys for big kids.

GCS8 and Ginsu

Physical Security; Make sure your building is "Butter Knife Proof"

Physical Security do's and don'ts on a budget. A humorous but intelligent look at a physical penetration done with the simplest of implements, a butter knife! With pictures and video, come see our two intrepid explorers as they physically compromise the security of their workplace, all the while discovering that a butter knife will cut swiss cheese security quickly and easily. Originally done as a lightning talk, the requests to do a full length talk poured in and led us to expand on it. Come laugh with us as we show you issues you are likely to encounter at your own office!

GCS8 is a mostly hardware-oriented person and loves to take things apart. He has an odd need to know how everything works, and has spent most of his life in front of a computer. His dad is a Ph.D from MIT, so growing up he always got amazing answers to anything he asked, was always encouraged to learn and was supplied with what he needed to do so. He's now a systems engineer who makes up projects at work to keep from getting bored.

Having grown up with a mother married to an IBM SE and a Unix guru father, Ginsu was bound to be a geek. Using DOS from age 4, he quickly figured out how to get around any and all attempts by his parents to limit his privileges, and by age 11 had been banned from AOL after being caught intruding into a mail server. By high school, he spent his leisure time writing fun programs to control the attendance and grade book systems, and was banned from the network 6 times in a row without being reinstated. After high school, he joined the Army to do FM radio communications, and spent most of 2008 in southern Iraq. He currently does Network/Systems Administration and lives with his fiancee Bri and their 11 cats.

SpikyGeek

Dealing with difficult co-workers: How I became the "Thanks for the candy" guy.

A set of war stories from the office dealing with annoying, disturbing, and sometimes downright crazy people on the job. A description of each event (names changed to protect the guilty), a post conflict analysis, a "what I SHOULD have said was" section, and perhaps even a lessons learned or method for others to avoid these circumstances. (This "thanks for the candy" setup was inspired by Dane Cook's bit about talking to the guy at the office no one talks to, so that he won't get shot later.)

Spiky is a computer geek that has been working in the security industry for over 10 years, with a diverse background covering IT, comms, crypto, programming, IA, and more. When not disturbing the proponents of appropriate comments, he can frequently be found listening to music to get fired by, changing his hair color frequently, or at home providing amusement and entertainment for his wife and two dogs.

Shane Lawson

Your business model is naked and ugly

We have a fair amount of academic arguments in the community when discussing vulnerabilities and exploits. That is great for the community and folks that enjoy the challenge, but not always very productive when trying to enact change for a more secure solution. This talk is focused more in an area that can drive actual change in one segment of business. I will use some real world examples, tell stories of how quickly

someone acts when you tell them their entire business model is completely flawed, and why understanding money and business can make you more successful. The talk will also show some interesting items that are freely available for all to view that the authors probably weren't expecting. The B2B systems we focused on are used by many large companies yet for some reason there has been very little published on their vulnerabilities. An overview of practical uses for the information will be delivered along with some easy protection methods.

Shane Lawson is the Director of Commercial and Federal Security Services for Tenacity Solutions, Inc. where he focuses on penetration testing, security assessments, and supply chain risk analysis for his clients. He previously served as a senior technical adviser and security analyst for the US Navy. Along with poking around on networks, Shane researches physical security systems and generally tries to break things with a focus on improvised and inexpensive tools. He is the technical editor for Deviant Ollam's Practical Lock Picking and Keys to the Kingdom.

Martin Bos & Eric Milam

Advanced Phishing Tactics Beyond User Awareness

Over the past 10 years, organizations have spent time, resources and considerable financial investments to protect their external perimeter from potential information security threats. Most advanced threat agents know if and when they bypass the hardened perimeter, successfully compromising assets within the internal environment is trivial, with very few controls in place to stop a focused and motivated intruder.

This talk will discuss why spear phishing penetration testing is a necessary exercise for all organizations. We will walk through and demonstrate live, our methodology that has proven extremely effective on numerous engagements. We will also focus on why advanced techniques should be used to assess internal user environments as a whole and that approaching a social engineering exercise as a user awareness exercise is not beneficial for an enterprise.

Eric is a senior security assessor on the Accuvant LABS enterprise assessment team with over fourteen (14) years of experience in information technology. Eric has performed innumerable consultative engagements including enterprise security and risk assessments, perimeter penetration testing, vulnerability assessments, social engineering, physical security testing, wireless assessments and extensive experience in PCI compliance controls and assessments. Eric is a project steward for the Ettercap project as well as creator and developer of the easy-creds and smbexec projects.

Martin Bos is a senior security assessor with the Accuvant LABS enterprise assessment team and has five (5) years of experience in the information technology industry. Martin specializes in black-box penetration testing, social engineering, physical security testing and enterprise network security assessments. Martin also has extensive knowledge in

performing wireless assessments. Martin Bos is a core developer of the BackTrack-Linux project and one of the founders of Derbycon. (Yay Derbycon!)

G. Mark Hardy

Keynote Address

G. Mark Hardy is founder and President of National Security Corporation. He has been providing cyber security expertise to government, military, and commercial clients for over 30 years, and is an internationally recognized expert who has spoken at over 250 events world-wide. G. Mark serves on the Advisory Board of CyberWATCH, an Information Assurance/Information Security Advanced Technology Education Center of the National Science Foundation.

A retired U.S. Navy Captain, he was privileged to serve in command nine times, including responsibility for leadership training for 70,000 Sailors. He also served as wartime Director, Joint Operations Center for US Pacific Command, and Assistant Director of Technology and Information Management for Naval Logistics in the Pentagon, with responsibility for INFOSEC, Public Key Infrastructure, and Internet security. Captain Hardy was awarded the Defense Superior Service Medal, the Legion of Merit, five Meritorious Service Medals, and 24 other medals and decorations.

A graduate of Northwestern University, he holds a BS in Computer Science, a BA in Mathematics, a Masters in Business Administration, a Masters in Strategic Studies, and holds the GSLC, CISSP, CISM and CISA certifications.

Jeff Brown

RE, CNO, Geopolitics, Oh My!

This session will delve into reverse engineering on a highly publicized piece of malware. A VMware image or ISO image will be made available to the attendees containing all the tools needed. I will step through obtaining static indicators from the file, peel back various wrappers, shellcode extraction and debugging of the code. This can be a good introduction for those who are interested in reverse engineering and seeing capabilities of those who manufacture said malware. Finally we'll tie everything together with a bit of social media and historical events.

Jeff Brown is the Director of Cyber Operations at Cyber Clarity, a United States consulting organization located in northern Virginia. Jeff has worked in various large scale security operations centers where he augmented analytical capabilities and provided trainings/ briefings on current cyber threats to their constituents. Previous experience include advancing analytics at US-CERT, briefings for the FS-ISAC, FIRST and various federal agencies as well as conducted training on current cyber threats to law enforcement and

SOC analysts across various sectors. He has developed curriculum and taught classes on information assurance for Regis University and in his spare time he experiments on a six string by applying various modes over major and minor scales.

Goto http://tinyurl.com/8qs57lm to download the ISO for this talk

Curtis Koenig

Insanely Great!

The only thing that never changes is change itself, but when is change good and needed and when is change for change sake? Ever wondered how people like Steve Jobs, Bill Gates and others were able to find important change and then lead it. We've all heard about managing changing, but what about leading change? What about focusing on the "Insanely Great!" and not merely on the mediocre. If you had the chance to attend "Knowing Where One's Towel Is" at the SDC'11 and you want to know more human / self hacker then this talk is for you. Come observe the "mostly hairless monkeys " with Curtis.

Curtis Koenig is currently a Security Minion (Sr. Security Program Manager) for Mozilla. His current focus is on the Security Lifecycle, with a goal of improving overall security quality in all Mozilla products. Curtis started his education and professional life in Microbiology, viruses of a different sort, and later moved back to his childhood passion of computers and security where he attempts to integrate his biological and scientific background to digital models. In his outside life Curtis works heavily with the Boy Scouts of America and youth of all ages to instill a love of the outdoors as well as teaching advanced leadership skills to adult leaders.

Lee Baird

Setting up BackTrack and automating various tasks with bash scripts.

I keep hearing about this BackTrack thang? What the heck is it, and why in the world do I need it? This presentation will walk you through the basics of setting up your VM, adding additional software and updating commonly used applications. From there, you will learn to automate various portions of a pentest with bash scripts.

Lee Baird works as a security consultant performing enterprise security assessments for Fortune 500 companies. He has a bachelors degree in accounting from Marshall University and is an Offensive Security Certified Professional.

5.

Bob Weiss & Benjamin Gatti

Cryptanalysis of the Enigma

Were Allen Turing to have survived to the present; he would have access to the most powerful computers and the liberty to choose his own friends: We note that he had neither; and yet it is significantly because of him, that we now have both. It is an honor to present a new Open Source software and a novel technique for cracking the Enigma cipher on the year of his Centennial.

As does Gillogy, Sullivan, Weierud, and other contemporary Enigma researchers, We apply Index of Coincidence in various forms over a subset of the parameter space, and promote a minority of results through a series of increasingly exhaustive tests. To this general approach we contribute two exploits: Stecker Isolation, which reduces the most complex module, the steckerbrett, from ~26^2 to 262 tests ; and Diagonal Conflation which prescribes a unique subset of the ringstellung by noting their inverse effect relationship with the message cipher.

We will attempt to break a message during the talk on a laptop. To improve performance we rely on OpenCL which provides cross platform access to GPU for General purpose computing.

More generally, we discuss the curve of entropy, complexity and the rapid improvement in computing power by showing that what took a national industrial effort to achieve in the 40's can now be superseded on a laptop computer.

Benjamin Gatti was born to hippies in the late 60's, grew up in California and taught himself electronics and software, traveled the World in the 90's, married abroad, and settled in Charlotte, North Carolina where he works as an independent software slacker. His hobbies include micro-controllers, music, sustainable energy & ecovillages, hackerspaces, atheism, activism, cooking, healing sick electronic appliances.

Bob Weiss is the founder of Password Crackers, Inc. (pwcrack.com) and a Defcon Goon. Bob spent his early career doing political and marketing work and lives with his family in Gaithersburg, Maryland.

Marcus J. Carey

Security Myths Exposed

The mission of the talk is to debunk information security myths. Many have speculated that some aspects of information security are myths. People ask: "Is information security a myth?", "Is this product bogus?, "Is my antivirus really that awesome?", or "Does the dark side have cookies?". All will be revealed at this talk.

Marcus J. Carey is a Security Researcher at Rapid7 with the Metasploit Engineering team. Marcus is well known for being a compulsive mentor in the information security community. Marcus has more than 18 years of experience in the information security field, working in the military, federal, and private sectors. Marcus served more than 8 years active duty in the U.S. Navy Cryptologic Security Group. Marcus ended his naval service by being assigned to the National Security Agency (NSA) where he engineered, monitored, and defended the Department of Defense's secure networks. Marcus earned a Master of Science in Network Security from Capitol College in Laurel, Maryland.

Dr. Noah Schiffman

Bioveillance: The Surreptitious Analysis of Physiological and Behavioral Data

Biometric security—"the something you are"—has become one of the largest growing areas of the security industry. The use of biometric authentication requires critical and irrevocable personally identifiable information. Developments in image acquisition techniques and advances in sensors allow one to remotely capture and collect human traits--a means of biometric surveillance. The constant acquisition, aggregation, and multi-modal fusion of physiological (facial recognition) and behavioral (gait analysis) biometric data create numerous vulnerabilities to personal privacy. Combined with affective computing, the subjective interpretation of one's intent is becoming a quantitative metric. This presentation will address new methods of non-cooperative biometric data acquisition, its use in behavioral categorization, and the subsequent threats posed to our privacy and individuality.

With 20+ years of industry experience, Noah Schiffman is a former hacker turned security consultant, specializing in pen-testing, threat assessment, and security integration. With degrees in cognitive psychology and mechanical engineering, he has worked on designing authentication/access control systems and improving security usability. After receiving a doctorate in medicine, his research and development have encompassed biometric technologies and medical device security. He has spoken at security conferences, such as ToorCon, InfoSeCon, CarolinaCon, and SOURCE Boston, and has been a frequent contributing writer for Network World and SearchSecurity.com. Currently, he is the CSO for a defense contractor in SC and an independent security consultant.

Carter Smith

Gangs and the use of Technology

Technology advances have changed the way the average American communicates, plans his or her day, shops, drives, and does many other things. Technology has changed the way criminals, specifically gang members, live their lives as well. As gangs evolve, many adopt more of a business model. How does that affect the way law enforcement should investigate them?

You will get an overview of criminal communications options, actions, and interactions followed by a discussion of how law enforcement – mostly gang cops – can and do respond. Ideas on how to engage, assist, or even thwart the detection of such activity will be provided. The use of metaphors to explain how technology functions often helps the not-so-literate grasp the concepts we will discuss – an impromptu brainstorming session on how that works will likely occur.

Carter F. Smith usually presents to groups that are wearing or sitting on badges. In his day job he is an Assistant Professor of Criminal Justice & Homeland Security in the Department of Public Management and Criminal Justice at the Internationally-renowned Austin Peay State University. During his more than twenty-two year career with the U.S. Army, he used a variety of lengthy titles to describe his jobs with the Criminal Investigations Command (CID). He has provided training on many gang-related topics to the TN, GA, FL, OK, and Northwest Gang Investigator's Associations, the Department of Defense, and the Department of Justice.

His research and investigative interests include military-trained gang members, technology use by gang members, and the intersection of criminal street gangs, organized crime, and terrorism. He's got a Ph.D from Northcentral University, a Juris Doctorate from Southern Illinois University - Carbondale, a Bachelor's degree from Austin Peay State University. He's been interviewed by a bunch of news outlets, has published a bunch on gangs, and was on two segments of the History Channel's Gangland series.

Scott Moulton

Hacking Your Credit Score; How the System is Flawed

Draw form his own recent experiences, Scott began monitoring his credit score daily and used this info to gain first-hand knowledge of how to work the system in his favor. Join us as we hear Scott's advice and lessons learned from dealing with credit agencies.

Scott Moulton is the owner of MyHardDriveDied.com. He is a Data Recovery Expert and Forensic Specialist. He is a veteran speaker at many conferences including OuterzOne, ShmooCon, DefCon, HackerHalted and SkyDogCon. His Data Recovery Courses provide industry leading expertise and are well known for their intensity.

Tyler Pitchford

Free-Source Litigation

Free-source is one of the greatest concepts of our time. There's little argument that it's changed not only the software industry, but also the world. Sadly, it's not all roses. When the dollars start flowing, ideals and principles often go out the door. Corporations form, licenses become suggestions, and lawsuits, inevitably, ensue. This is our topic.

We're not going to focus on just the gloom-and-doom end game; instead, we're going to try and cover the entire spectrum. We'll cover getting your project setup under a free-source license, navigating the twisted roads of intellectual-property rights (and wrongs), and, of course, what to expect if everything ends up in court. What do courts think of free-source licenses? What support is available out there? And, most importantly, what can you do about it all?

As with anything legal, there's a lot of grey. Straight answers are a rare commodity, and unanswered questions abound. But despite all the mystery, there are some answers, some suggestions, and an abundance of good practices to be had. We'll cover as many of them as we can.

Tyler holds a bachelor of arts in Software Systems Design from New College of Florida, a Juris Doctor from the Stetson University College of Law, and is licensed to practice law in Florida. He co-founded the Azureus Bittorrent client in 2003, and currently works as an appellate attorney at Brannock & Humphries (http://www.bhappeals.com),
focusing on mass-tort litigation and appeals. While in the software industry, he worked as anything from a bit-twiddler an executive. As for the legal world, he's worked at the Florida State Attorney's office, the United States District Court for the Middle District of Florida, and the Florida Supreme Court. Tyler has also presented on various infosec and the legal topics around the country (SkyDogCon, PhreakNIC, Defcon, OuterzOne, ToorCamp, Shmoocon, and the AirForce), and taught several courses on computer programming and security throughout the years. One day he'd like to take a vacation; he's heard they're nice.

Billy Hoffman

Lessons Learned founding and running a Startup

In 2009, I left a successful career in the computer security industry to start a web performance company. I've done a lot of things wrong, some things right, and learned quite a bit along the way. I'll share my experiences, provide some advice, and explain why all of the skills and traits that make you an excellent hacker work against you when trying to start and run a small company.

Billy Hoffman is the founder and CEO of Zoompf. Prior to Zoompf, Billy worked as a security researcher for SPI Dynamics, a web security scanner vendor. Following it's acquisition by Hewlett Packard in 2007, Billy managed HP's Web Security Research Group. He has spoken at web performance and security conferences around the world, published the book Ajax Security with Addison Wesley, and is currently writing a book on web performance for No Starch Press.

Alex Kirk

Lifecycle and Detection of an Exploit Kit

As the process of owning systems and dragging them into botnets becomes ever more commercialized, exploit kits have emerged as a favorite of attackers; their point-click-own nature means even non-technical people with a little cash can control your PC today. This talk will examine how some popular exploit kits work, from lure through payload; and discuss detection and prevention methodologies, with a focus on IDS/IPS. Live examples from the wild will be used throughout.

Alex Kirk is a senior researcher with the Sourcefire Vulnerability Research Team (VRT), and the head of that group's Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) program, which is designed to increase direct collaboration between Sourcefire customers, the Snort user community, and the VRT in the interests of improved detection and coverage. In his 8 years with the VRT, Alex has become one of the world's leading experts on Snort rules, and has honed skills in reverse engineering, network traffic analysis, and systems security. He recently contributed a pair of Snort-related chapters to "Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century," and is a regular contributor to the widely-read VRT blog (http://vrt-sourcefire.blogspot.com/). His current major technical project at Sourcefire involves automated collection of network data generated by malicious binaries, including Android packages, and analysis of that data for detection purposes.

Points of Interest

Here is some information on nearby areas which may be helpful while you attend the conference:

Conference Hotel
The conference is held at the Hotel Preston. Put this address in your phone so If you get lost wandering around the city you can get back:

Hotel Preston
733 Briley Parkway
Nashville, Tennessee 37217

The Hotel Preston is centrally located 5 minutes from most everything.
Free Airport and close-in Shuttle Service and Complimentary parking. They will take you to a few choice locations but Las Vegas is out of their range.

The Hotel Preston features Cafe Isabella, dine where the SkyDogCon staff has eaten lunch about once a week for the past year! Need suggestions? See a core team staff member. Little pink bunnies are not on the menu.

Visit the funky bar, The Pink Slip, for your favorite libations! One of ours is Maker's Mark on the rocks.

At some point you might need to get your hardware hack on and need some parts that are not in the hardware hacking village. The closest electronics store is:

Radio Shack
55 East Thompson Lane
Nashville, TN 37211
(615) 445-3151

Sometimes people forget to pack sundry items or just decide to be benignly mischievous. If you need threads, kicks, trainers, specs, boats, ATVs or pretty much anything else you can get at a mall with 100+ stores.

Opry Mills Mall
433 Opry Mills Drive
Nashville, TN 37214

At some point you may be overloaded with hacking and just want to chill under a planetarium screen. Nashville has a great science center.
Adventure Science

800 Fort Negley Blvd
Nashville, TN, 37203
www.adventuresci.com

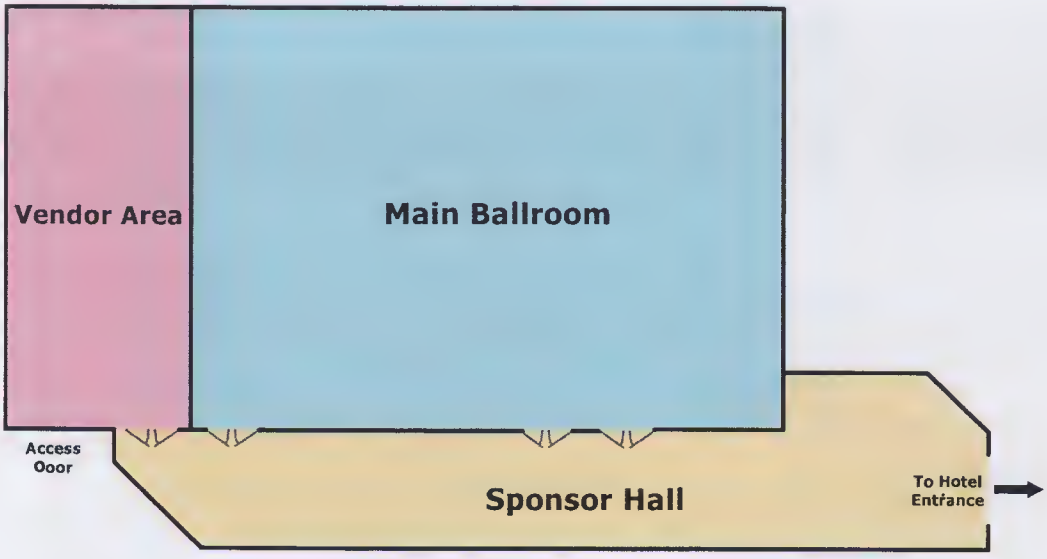
We do recommend Cafe Isabella, but if your arteries need some more grease and you have a car, there is plenty of fast food one interstate exit North on Briley Parkway at Donelson Pike.

THANK YOU

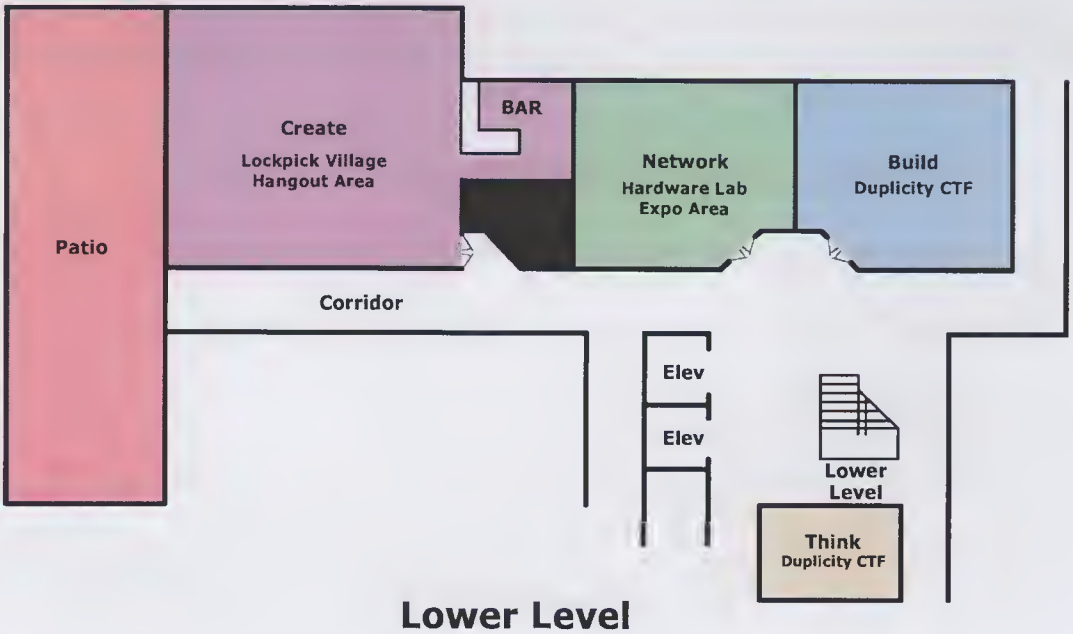
Thank you for helping us bring a technical security conference to our Mid-South Community. We believe that in order for us to continue to thrive as a culture we must embrace a wide variety of ideas and approaches. We must continue to reach out to one another to help our group flourish. We thank the speakers who carved time out of their "normal" lives to come here and share their knowledge with us. We thank the volunteers who gave up their sleep, their time (and in one case an appendage), to bring together an event that they believe in. We also are thankful for all of our participants, we thank you for coming and attending, as without you there would be no con. We ask that all of you keep the spirit of brotherhood alive. Reach out to your fellow attendees! Exchange <electronic communication of your choice here> and support and mentor one another until we meet again!

Thank you! We hope to see you all again next year!

-SkyDog & MrsSkyDog



Lobby Level



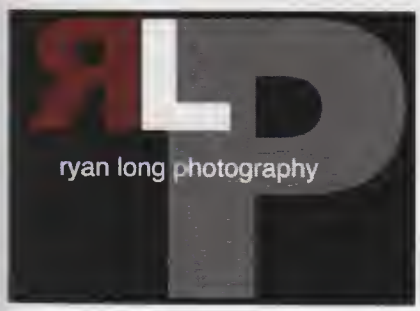
Lower Level

SPONSORS


nPULSE
TECHNOLOGIES


SE Solutions
strategic solutions for the enterprise


mozilla


RLP
ryan long photography


APEX
Systems, Inc.


Cyber
Clarity


JUNIPER
NETWORKS


hp


ForeScout


ROKABEAR
HOSTING SERVICES


QUALYS
ON DEMAND SECURITY


FOOLS


immixGroup


SOURCEfire


McAfee
An Intel Company


Guidance
SOFTWARE


zOompf


VICIOUS DATA RECOVERY


no starch
press


THE
Funky
Umbrella


My
Hard
Drive
Died
mhdd